Written Statement of:

John G. Palfrey, Jr.
Clinical Professor of Law & Executive Director
Berkman Center for Internet & Society, Harvard Law School

Congressional Human Rights Caucus Members' Briefing
on the subject of human rights and the Internet in China
February 1, 2006

Mister Chairman, Distinguished Members of the Caucus:

My name is John Palfrey. Thank you for the leadership of this Caucus in drawing attention to the relationship between the Internet and human rights in China and for the opportunity to speak with you today. I am here today as a member of a team of researchers, called the OpenNet Initiative, that has been conducting empirical testing of China's Internet filtering regime for the past several years and monitoring the involvement of United States companies in that regime. My colleagues Ronald Deibert of the University of Toronto, Rafal Rohozinski of the Advanced Network Research Group of the Cambridge Security Program, University of Cambridge, and Jonathan Zittrain of the University of Oxford and Harvard Law School, are also principal authors of the OpenNet Initiative's work. We have also studied in depth the filtering regimes of states in the Middle East, the former Soviet republics, and parts of East Asia. I am joined today by my colleague Nart Villeneuve, the Director of Technical Research at the Citizen Lab at the University of Toronto.

Today the Caucus considers human rights with respect to the Internet in China. I applaud your efforts to shine a spotlight on this important matter. I hope that your efforts, and those of your colleagues, will lead to new ways to work together to achieve our common goal of global economic development that is consistent with the values that we hold dear as Americans and as citizens of our increasingly connected world.

While China seeks to grow its economy through use of new technologies, the Chinese state's actions suggest a deep fear of the sometimes disruptive effects of free and open communications made possible by the Internet – particularly on topics of human rights. This fear has led the Chinese government to create the world's most sophisticated Internet filtering regime. One of the topics commonly blocked is information related to human rights, including the website of the respected NGO, Human Rights Watch.

Increasingly, the Chinese state has turned to private companies that control parts of the middle of the network to assist in its filtering and surveillance practices. These companies find themselves today in an awkward, if not untenable, position on this issue of ethics and human rights. Individual companies can be isolated and pressured by the

filtering state and undercut by competitors willing to comply with surveillance and filtering requests.

United States technology companies, which have led the Internet revolution from the start and have brought us many of its extraordinary benefits, are now in the uncomfortable posture of helping to carry out Internet filtering practices. These companies also find themselves under pressure to turn over sensitive personal information to law enforcement officials, in circumstances where these companies would not turn over the information here in the United States.

Private technology companies cannot today participate in these marketplaces without consequences based upon their actions. Human rights are implicated. Companies in this position have an obligation to figure out what it means to act ethically when they are doing business in a place like China. They also have a self-interest in having a common code of practice to which they can point and rely upon in resisting abusive filtering and surveillance requests. The United States Congress is right to pay attention.

Despite what may seem to be a common set of problems, United States technology companies should not be lumped into a single category when it comes to their participation in Internet filtering and surveillance practices. Plainly, there are different issues at stake when a company is making technology products that are designed to carry out filtering regimes in other countries around the world as compared to a company that is making general-purpose technology that happens to be used to filter or spy on Internet-based communications. Surely there are differences between the company that offers a limited online service in China and collects no personally identifiable data as compared to a company that not only collects large amounts of such data but turns it over prior to a formal legal action. Surely we would distinguish between a company that folds at the first hint of controversy and the company that draws lines in the sand and puts its license to do business in that state in harm's way. There are ethical lines to be drawn between various kinds of technology companies that are doing business in China. These lines will help to shape what we believe to be good public policy on this matter.

In terms of how to move forward, there are several options.

First, and most appealing as a next step, is for the United States information technology industry, perhaps with other players from states that face this problem, to work together to try to sort out a common ethical pathway. I, and some of my colleagues at the Berkman Center at Harvard Law School, believe that we should explore the development of a set of principles that would guide businesses that are offering services in states that filter extensively and spy on Internet conversations and give them a base of support for resisting abusive surveillance and filtering requests.

There are a number of things that United States technology companies can do to make their actions more transparent to users, more protective of civil liberties, and more accountable to all of us. Yesterday, Microsoft announced a policy with respect to content hosted on their popular MSN Spaces blog software in China, which is very much a step in the right direction.

The Chinese state's filtering systems lack transparency in nearly every sense. In addition to limiting what Chinese citizens can come to know about the censorship process, this lack of transparency complicates the task of monitoring its filtering regime.

Most important, this lack of transparency contributes mightily to the climate of self-censorship. Chinese officials very rarely admit that the state censors Internet content. Officials do not disclose at any level of granularity what material it targets through the filtering regime. United States technology companies can help on this transparency front by how they carry out their blocking.

Second, it may be the case that the Congress could develop a corollary to the Foreign Corrupt Practices Act that would guide – and tie the hands of – United States technology companies doing business under these circumstances. Such a step is risky on many levels and should be taken only with great care, and only if our technology industry is unable to work out the problem on its own.

Third, the United States ought to consider making this human rights issue a matter of foreign trade policy or other forms of international negotiation. In the Internet context, the United States ought to stop worrying about the future of the Internet Corporation for Assigned Names and Numbers and should make Internet filtering and surveillance the key Internet governance issue on the world stage.

The best outcome is not to ban the involvement of United States technology companies in China outright. The best outcome would be for our technology companies to be able to compete in these marketplaces – with their best-in-the-world offerings – without having to compromise our values and without having to become complicit in Internet censorship and surveillance.

In conclusion, we ought to see this issue not as a crisis, but rather as an opportunity. Internet technologies, developed by the likes of Microsoft, Yahoo!, Google, Cisco, and many others, are doing terrific things for democracy around the world. At the same time, the People's Republic of China's Internet filtering and surveillance regime has the greatest effect on the freedom of expression, and on the efforts of human rights workers, of any filtering regime throughout the world.

We need to come together to figure out how to ensure that these companies and their technologies are indeed a force for greater democratic participation, not pushing against it. These companies should be, and can be, the darlings of the human rights community for what they can do for human rights in places like China. It doesn't happen to be the case today, but I have no doubt that we can get to that point through collaboration that is grounded in honesty, openness, and transparency.

-- End of Written Testimony --

Appendix:

The OpenNet Initiative's Methodology for Studying Internet Filtering in China.

Members of our consortium have been collecting data on China's Internet filtering regime since 2002. The data included in this report have been updated as recently as this week. As the Chinese government has developed more sophisticated means of filtering, we too have developed more sophisticated and comprehensive means of testing their filtering efforts. Since our last study, our testing methods have become substantially more fine-grained and reliable.

To gauge how Internet filtering likely affects the average Chinese Internet user, ONI employs a variety of means to test blocking and censorship and to ensure data integrity. We test filtering from different points on China's network, in different geographic regions, across time. The resulting data allow us to conduct rigorous longitudinal analysis of Internet blocking in China. We examine both the response that users receive from the network and from the Web servers involved and information about the route that a request takes on its way from a user to a Web server – allowing us to pinpoint exactly where information is censored and controlled. While it is impossible to paint a flawless picture of China's Internet filtering efforts at any given time, we are increasingly confident that our data present an accurate snapshot of China's Internet filtering regime today.

We have tested China's Internet filtering regime using four methods. Under Nart Villeneuve's leadership, ONI developed and deployed an application to test within China what content is, and is not, blocked by the state's system. Volunteers installed and ran this application on their home computers to allow ONI to probe China's filtering from a wide range of access points inside the country. Our volunteers also ran manual checks for access to web sites.

Second, we accessed proxy servers in China to duplicate and augment this in-state testing of whether or not a citizen could access a certain web site. Proxy servers are points in China's network that act to aggregate and respond to user requests for content. Accessing a proxy server in China allows ONI to browse the Internet as though we were in China, even though we are physically located in another country. Through proxies, we are able to obtain a random sampling of Web content – and censorship – across multiple networks and service providers.

We have also explored whether China blocks other types of Internet-related communications. Anecdotal evidence has suggested for a long time that China blocks certain e-mail communications and that Web logs – or "blogs", which are personal online journals, often kept by increasingly famous activists – have been more recently targeted by the Chinese government for blocking.

To test these hypotheses, we published content on blogs on three of China's most popular blog providers to evaluate the services' keyword filtering mechanisms. We then later sought to access this blog content that we had published.

Finally, we sent a series of test e-mail messages to, and from, accounts hosted by several Chinese ISPs. These messages contained content on sensitive topics – such as political dissidents, objections to the state's repression of the Tiananmen Square

protests, and religious persecution – typical of e-mails sent by human rights organizations.

In addition to employing these technical methodologies, we have closely studied the legal and policy regimes in place in China. The insights of many scholars and activists, both inside China and elsewhere, guided our research and provided quality assurance.

Topics Censored by the Chinese Filtering Regime.

China filters Internet content on a broad array of topics. The censors particularly target sensitive political topics for blocking. To determine precisely what is blocked, we created a keyword list of terms on sensitive topics, such as the Falun Gong spiritual movement, the Taiwanese independence movement, and criticism of China's government and leaders. We used the Google search engine to compile a list of large numbers of sites related to these keywords. Our volunteers then attempted to access these sites from within China using our testing application.

Some of the most noteworthy of the topics censored include:

- Information online related to opposition political parties (more than 60% of Chinese-language sites tested were blocked);

- Political content (90% of Chinese-language sites tested on *The Nine Commentaries*, a critique of the Chinese Communist Party, and 82% of sites tested with a derogatory version of Jiang Zemin's name were blocked);

- The Falun Gong spiritual movement (44 – 73% of sites tested, in both English and Chinese languages);

- The Tiananmen Square protest of June 4, 1989 (at least 48% of Chinese-language sites tested, and 90% of sites related to the search term "Tiananmen massacre");

- Independence movements in Tibet (31% of tested Chinese-language sites), Taiwan (25% of tested Chinese-language sites), and Xinjiang province (54% of tested Chinese-language sites); and,

- Virtually all content on the BBC's web properties and much of the content published online by CNN.

China has issued official statements about its efforts to limit access to Internet pornography. However, we found that less than 10% of sites related to searches for the keywords "sex," "pornography," and "nude" were blocked. This imprecision, when compared either to the effectiveness of China's censoring of political content or to the relatively thorough blocking of pornographic materials by states in the Middle East, suggest that blocking pornography is nowhere near the imperative that controlling political speech is in China. It also suggests that China's war on pornography may be focused more on closing domestic sources of pornography than on filtering foreign sites that are providing pornographic content.

Our testing also found evidence that China tolerates considerable overblocking – filtering of content unrelated to sensitive topics, but located at URLs or with keywords similar to these subjects – as an acceptable cost of achieving its goal of controlling Internet access and publication. China has managed over time to reduce the rate of overblocking as its filtering technologies have improved.

Types of Communications Affected by China's Filtering Regime.

China's commitment to content control is revealed by the state's efforts to implement filtering for new methods of communication as they become popular. Most states that filter the Internet do an ineffective job of blocking access to certain web sites, and stop there.

While China's blocking of World Wide Web sites is well-known, much less is known about the extent to which China blocks other forms of Internet-based communications. As Web logs ("blogs") became popular in 2004, the state initially closed major Chinese blog service providers until they could implement a filtering system. When these providers re-opened, their service included code to detect and either block or edit posts with sensitive keywords. Similarly, on-line discussion forums in China include both automated filters and human Webmaster inspections to find and remove prohibited content. Most recently, China moved to limit participation in university bulletin board systems (BBS) that had featured relatively free discussion and debate on sensitive topics. The Chinese filtering regime also causes the blockage, or dropping, of e-mails that include sensitive terms. Our testing of e-mail censorship suggests that China's efforts in this area are less comprehensive than for other communications methods, though reports from the field suggest that the fear of surveillance and blockage of e-mails is a serious issue for many activists regardless of the precise extent of the censorship itself.

One of the most intriguing questions, as yet unanswered, is whether emerging new technologies will make Internet filtering harder or easier over time. A new, emerging crop of more dynamic technologies – centered on the fast-growing XML variant RSS, which is a means of syndication and aggregation of online content, such as weblog entries and news stories from major media outlets – should make filtering yet harder for the Chinese and for other countries that seek to control the global flow of information. The cat-and-mouse game will continue.

The Legal Context of Filtering in China.

China's intricate technical filtering regime is buttressed by an equally complex series of laws and regulations that control the access to and publication of material online. While no single statute specifically describes the manner in which the state will carry out its filtering regime, a broad range of laws – including media regulation, protections of "state secrets," controls on Internet service providers and Internet content providers, laws specific to cybercafés, and so forth – provide a patchwork series of rationales and, in sum, massive legal support for filtering by the state. The rights afforded to citizens as protection against filtering and surveillance, such as a limited privacy right in the Chinese Constitution, which in other situations might provide a counter-balance against state action on filtering and surveillance, are not clearly stated and are likely considered by the

state to be inapplicable in this context. For the most part, the Chinese legal regime is not transparent, in the sense that it does not describe the filtering regime.

Our analysis of China's legal regime indicates a significant expansion in the number of statutes, regulations, and regulatory bodies involved in oversight and control of Internet access and content since 2000. These rules often appear to be arbitrary and are certainly extraordinarily burdensome, such as rules that call for multiple licensing and registration requirements imposed upon Internet content providers.

China's legal system imposes liability for prohibited content on multiple parties: the author who creates it, the service provider who hosts it, and the end user who accesses it. This combination of transaction costs and broad liability has a substantial chilling effect on on-line communication.

We are cognizant that, while we have taken great care in our legal analysis of China's filtering regime as it appears on the books, our report may not describe the law as it applies on the ground. Political stability is clearly more important than legal justification for the state's actions, as a comparison of China's filtering regime to the corresponding legal framework demonstrates.

A Comparison of China with Other States that Filter.

Our studies have compared the Internet filtering practices of a series of national governments in a systematic, methodologically rigorous fashion. A primary goal of this research is to reach useful, substantive conclusions about the nature and extent of Internet filtering in states that censor the Internet and to compare practices across regions of the world. Over the course of the next several months, we will release a series of extensive reports that document and provide context for Internet filtering, previously reported anecdotally, in each of the dozen or so countries that we have studied closely. The new reports released to date – which document filtering in Saudi Arabia, the United Arab Emirates, and Bahrain as well as in China – will be followed shortly by other studies of other states in the Middle East, East Asia, and Central Asia.

Filtering regimes – and their scope and level of effectiveness, respectively – vary widely among the countries we have studied. Filtering is practiced at some level by most countries; it is best thought of as a continuum of behavior rather than a binary, on-off approach to content control. Some countries employ only symbolic filtering, and depend on legal or social pressures to constrain content. These states include Bahrain and Singapore, which block only a few sites that are primarily pornographic in nature. Other countries demonstrate limited blocking but, because of an unsophisticated approach to filtering, also censor large numbers of unrelated sites. This inadvertent filtering, known as "overblocking," was demonstrated by South Korea when it sought to prevent access to sites promoting North Korea. Finally, many countries employ a mix of commercial software (from American companies such as Secure Computing and Websense) to control content such as pornography and gambling while also customizing their block lists to target prohibited political, religious, and social content.

China, as documented in a number of studies and supported by the our findings, institutes by far the most intricate filtering regime in the world, with blocking occurring at multiple levels of the network and covering content that spans a wide range of topic areas. Though its filtering program is widely discussed, Singapore, by contrast, blocks

access to only a small handful of sites, mostly pornographic in nature. Most other states that we are studying implement filtering regimes that fall between the poles of China and Singapore, each with significant variation from one to the next. These filtering regimes can be properly understood only in the political, legal, religious and social context in which they arise.

A complete study of Internet filtering in China, as of 2005, may be found at http://www.opennetinitiative.net/china/.

The OpenNet Initiative is a collaborative partnership between three leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet & Society at Harvard Law School; and the Advanced Network Research Group at the Cambridge Security Programme, University of Cambridge.